UNITED STATES DISTRICT COURT
DISTRICT OF SOUTH DAKOTA
SOUTHERN DIVISION

UNITED STATES OF AMERICA, Plaintiff, vs. ERIC WALLACE HEDRICK, Defendant.	CR19-40051 GOVERNMENT'S RESPONSE TO DEFENDANT'S MOTION TO SUPPRESS EVIDENCE

Eric Hedrick ("Hedrick") made a motion to suppress evidence obtained with a search warrant. (Doc. 20). The United States resists the motion.

FACTS

In this case, three search warrants were obtained. The Defendant attacks the first one claiming the agent willfully misled the reviewing Court. If successful with his challenge, the Defendant seeks to suppress evidence obtained from the subsequent search warrants as fruit of the poisonous tree. (Doc. 20).

The first search warrant was obtained on January 17, 2019. An affidavit was submitted and signed, under oath, by Homeland Security Investigations Special Agent Charla Aramayo. The purpose of the search warrant was to open and access a digital file suspected of containing child pornography. The file was sent to the South Dakota Division of Criminal Investigation by Google as part of a Cybertip to the National Center for Missing and Exploited Children (NCMEC). The Affidavit in Support of Search Warrant Application was filed under seal as

part of the Defendant's Motion to Suppress as Attachment 1. It will be referred to in this Response as "Affidavit" with references to specific numbered paragraphs.

The Affidavit – January 17, 2019

In her Affidavit, Agent Aramayo established probable cause. She was seeking a warrant "to open and view an image of *suspected* child pornography" that was "associated with CyberTipline Report 43517337." (Affidavit, ¶ 3). Agent Aramayo explained that the origin of the investigation began when "Google, an electronic service provider (ESP), provided an uploaded image of *suspected* child pornography through CyberTipline Report 43517337 to NCMEC." (Affidavit, ¶ 8). After the image of suspected child pornography was sent to NCMEC, NCMEC provided the content of the uploaded image to the South Dakota Internet Crimes Against Children (ICAC) Task Force." (Affidavit, ¶ 8). Agent Aramayo explained that the image suspected of being child pornography "has not yet been viewed by HSI." (Affidavit, ¶ 8).

In her Affidavit, Agent Aramayo also explained the process for companies to report possible child pornography. "Companies that suspect that child pornography has been stored or transmitted on their systems can report that information to NCMEC in a cybertip." (Affidavit, ¶ 9). Once NCMEC has the report and the information provided by the Internet Service Provider (ISP) or Electronic Service Provider (ESP), NCMEC attempts to locate where the activity

occurred and sends the cybertip to law enforcement in the appropriate jurisdiction. (Affidavit, ¶ 10).

Agent Aramayo then explained the Cybertip made by Google. CyberTip 43517337 was made by Google on November 24, 2018, and included a file, "the content of which NCMEC did not review." (Affidavit, ¶ 12). Agent Aramayo further explained, "[t]he report indicated the contents of the file were not reviewed concurrently to making the report, historically a person had reviewed a file whose hash (or digital fingerprint) matched the hash of the reported image and determined it contained apparent child pornography." (Affidavit, ¶ 12). This description is a verbatim recitation of NCMEC's CyberTipline Report, page 3. (Defendant's Motion to Seal, Attachment 2, bate stamp 0032).

Agent Aramayo also explained the process that ESPs and ISPs use to identify images or files suspected of child pornography. The process involves the comparison of "hash values." A "hash value" is "akin to a fingerprint for a digital file." (Affidavit, ¶ 13). NCMEC maintains a database of images identified by NCMEC or law enforcement as child pornography, and the corresponding "hash values" of the images. (Affidavit, ¶ 13). The list of "hash values" are available to ISPs and ESPs to compare to the hash values of all files transmitted by customers on their systems. (Affidavit, ¶ 14). "If the ISP or ESP finds that a hash value of a file on its systems matches one on the list, it captures the file along with information about the user who posted, possessed, or transmitted it on the

ESP's or ISP's systems and submits the information to NCMEC as a cybertip." (Affidavit, ¶ 14).

Agent Aramayo stated that "the ISP and ESP use PhotoDNA." She described PhotoDNA as a technology that "was used to determine that a user of its services posted or transmitted a file with the same hash value as an image that has previously identified as containing child pornography." (Affidavit, ¶ 15). Lastly, Agent Aramayo stated that the probable cause was based on the hash value comparison of the file in custody with files previously identified as child pornography. (Affidavit, ¶ 16).

Legal Analysis

I. Information in the Affidavit established probable cause for a search warrant to be issued.

A. The Affidavit is Truthful and Accurate.

Following issuance of a search warrant, "'only that information which is found within the four corners of the affidavit may be considered in determining the existence of probable cause.'" *United States v. Solomon*, 432 F.3d 824, 827 (8th Cir. 2005). The affidavit "should be examined under a common sense approach and not in a hypertechnical fashion." *Id. (*quoting *United States v. Williams,* 10 F.3d 590, 593 (8th Cir.1993)). Probable cause requires, "only a probability or substantial chance of criminal activity, not an actual showing of such activity." *United States v. Neumann*, 183 F.3d 753, 756 (8th Cir. 1999).

In her Affidavit, Agent Aramayo, stated more than one time that the image was *suspected* of being child pornography. She accurately stated that Google

suspected the file to contain child pornography, (Affidavit, ¶ 8), HSI never viewed the file, (Affidavit, ¶ 8), and that NCMEC did not review the file. (Affidavit, ¶ 12). At no place in her Affidavit did Agent Aramayo assert that anyone in the chain of custody of the file to be searched had viewed the file to verify that it was child pornography.

The Defendant's entire argument is based on a misunderstanding of the "hash value" comparison process that Agent Aramayo accurately and truthfully described in her Affidavit. ISPs do not physically look at files to report the transmission of child pornography. The volume of internet traffic would make such a process impossible. Instead, an automated process has been created that allows ISPs, such as Google, to scan and compare "hash values" of files of images previously identified as child pornography. *United States v. Reddick*, 900 F.3d 636, 637 (5th Cir. 2018). This technology was developed to help detect the illegal trafficking of child pornography. When there is a match of hash values, the ISP generates a report and sends to NCMEC.[1] *United States v. Stevenson*, 727 F.3d 826, 828 (8th Cir. 2013).

The software known as "PhotoDNA" is a program developed by Microsoft that computes and compares hash values. In her Affidavit, Agent Aramayo explained that the technology of comparing hash values had been used by Google "to determine that a user of its services posted or transmitted a file with *the same*

[1] ISPs that have information about an apparent violation of federal child pornography laws are required to provide a CyberTip to NCMEC, pursuant to 18 U.S.C. § 2258A.

hash value as an image that has previously identified as containing child pornography." (Affidavit, ¶ 15). This was a truthful and accurate statement of fact. Further, when compared to the NCMEC CyberTip report, there is no contradiction as the Defendant claims. The NCMEC report stated that, "the contents of the file were not reviewed concurrently to making the report." Agent Aramayo provided this exact phrase to the reviewing Court in paragraph 12 of her Affidavit. To claim that it was omitted is a misstatement of the contents of the Affidavit.

Agent Aramayo further accurately and truthfully quoted the NCMEC CyberTip Report where it declared, "[t]he report indicated the contents of the file were not reviewed concurrently to making the report, historically a person had reviewed a file whose hash (or digital fingerprint) matched the hash of the reported image and determined it contained apparent child pornography." (Affidavit, ¶ 12). This hash value comparison was provided in the NCMEC CyberTip and truthfully and accurately described in the Affidavit. Therefore, there were no false or misleading statements, or omissions, in the Affidavit.

B. No basis for a *Franks* hearing.

An affidavit supporting a search warrant is presumed to be valid. *United States v. Neal*, 528 F.3d 1069, 1072 (8th Cir. 2008) (citing *Franks v. Delaware*, 438 U.S. 154, 171 (1978); *United States v. Snyder*, 511 F.3d 813, 816 (8th Cir. 2008)). "Probable cause exists when a 'practical, common-sense' inquiry that considers the totality of the circumstances set forth in the information before the

issuing judge yields a 'fair probability that contraband or evidence of a crime will be found in a particular place.'" *United States v. Stevens*, 530 F.3d 714, 718 (8th Cir. 2008) (citing *Illinois v. Gates*, 462 U.S. 213, 238 (1983)). As the United States Supreme Court stated:

> [A]ffidavits for search warrants, such as the one involved here, must be tested and interpreted by magistrates and courts in a common sense and realistic fashion. They are normally drafted by nonlawyers in the midst and haste of a criminal investigation. Technical requirements of elaborate specificity once exacted under common law pleadings have no proper place in this area. A grudging or negative attitude by reviewing courts toward warrants will tend to discourage police officers from submitting their evidence to a judicial officer before acting.

United States v. Ventresca, 380 U.S. 102, 108 (1965).

In this case, the Defendant has challenged the validity of the affidavit used to support a federal search warrant to search a file that was reported by Google to NCMEC. To obtain a hearing, this type of challenge requires the defendant to meet the strict requirements of *Franks v. Delaware*, 438 U.S. 154 (1978). It is not necessary for this Court to grant every request for a *Franks* hearing to challenge the validity of an affidavit used to support a search warrant. "In order to receive a hearing on a defective warrant issue, the defendant must make some preliminary showing that the warrant application contained false statements or omissions that were material to the finding of probable cause." *United States v. Oleson*, 310 F.3d 1085, 1090 (8th Circuit 2002) (upholding the denial of a request for a *Franks* hearing) (citing *Franks*, 438 U.S. at 164). Further, a defendant must first meet his burden of submitting an offer of proof that

supports the defendant's claim that the affidavit contains statements that are knowingly false or made with a reckless disregard for the truth. The type of showing required is not easily met. *United States v. Milton*, 153 F.3d 891, 896 (8th Cir. 1998).

In *Franks v. Delaware*, the United States Supreme Court described when a hearing is necessary as follows:

> There is, of course, a presumption of validity with respect to the affidavit supporting the search warrant. To mandate an evidentiary hearing, the challenger's attack must be more than conclusory and must be supported by more than a mere desire to cross-examine. There must be allegations of deliberate falsehood or of reckless disregard for the truth, and those allegations must be accompanied by an offer of proof. They should point out specifically the portion of the warrant affidavit that is claimed to be false; and they should be accompanied by a statement of supporting reasons. Affidavits or sworn or otherwise reliable statements of witnesses should be furnished, or their absence satisfactorily explained. Allegations of negligence or innocent mistake are insufficient. The deliberate falsity or reckless disregard whose impeachment is permitted today is only that of the affiant, not of any nongovernmental informant. Finally, if these requirements are met, and if, when material that is the subject of the alleged falsity or reckless disregard is set to one side, there remains sufficient content in the warrant affidavit to support a finding of probable cause, **no hearing is required**. On the other hand, if the remaining content is insufficient, the defendant is entitled, under the Fourth and Fourteenth Amendments, to his hearing. Whether he will prevail at that hearing is, of course, another issue.

Franks, 438 U.S. at 171-72. (emphasis added).

The Defendant has alleged that information contained in paragraphs 15-16 is false. Specifically, the Defendant asserts that the information provided in these paragraphs of the Affidavit is "materially misleading, if not outright false." (Memorandum, p. 2). As the Government argued above, there are no

misstatements of fact in Agent Aramayo's Affidavit and a *Franks* hearing is not necessary.

However, in the event the Court were to determine there is some question about the accuracy of some factual assertions in the Affidavit, it has repeatedly been held that proof of negligence or an "innocent mistake" does not establish a *Franks* violation. *Neal*, 528 F.3d at 1072 (citing *Franks*, 438 U.S. at 171 ("Allegations of negligence or innocent mistake are insufficient"); *Snyder*, 511 F.3d at 816 ("Allegations of negligence or innocent mistake will not demonstrate reckless or deliberate falsehood")). In the Eighth Circuit, affidavits used to support search warrants have been upheld as valid even when they contain inaccurate statements. *United States v. Clapp*, 46 F.3d 795, 800 (8th Cir. 1995). In *Clapp*, the affiant stated in his affidavit that he participated in the interview of a witness. Instead, the affiant had actually overheard the interview from across the room. *Id.* at 799-800. In the *Clapp* decision, the court found that the affiant's statement in the affidavit was "misleading and, thus, was negligent; it was not reckless, however." *Clapp*, 46 F.3d at 801.

Other courts, in defining the term "reckless disregard for the truth" have looked to what the affiant "believed or appropriately accepted" as true. *Clapp*, 46 F.3d at 800 (citing *United States v. Lueth*, 807 F.2d 719, 725 (8th Cir. 1986); *United States v. Luschen*, 614 F.2d 1164, 1172 (8th Cir. 1980), *cert. denied*, 446 U.S. 939 (1980)). In *Franks,* 438 U.S. 154, the Court stated:

> When the Fourth Amendment demands a factual showing sufficient to comprise "probable cause," the obvious assumption is that there

> will be a *truthful* showing. This does not mean "truthful" in the sense that every fact recited in the warrant affidavit is necessarily correct, for probable cause may be founded upon hearsay and upon information received from informants, as well as upon information within the affiant's own knowledge that sometimes must be garnered hastily. But surely it is to be "truthful" in the sense that the information put forth is believed or appropriately accepted by the affiant as true.

Franks, 438 U.S. at 165.

In this case, the Affiant, Agent Aramayo, relied on her training and experience and the information she obtained in the NCMEC CyberTip report. Based on the totality of the circumstances, Agent Aramayo "believed and appropriately accepted" that the hash value of the suspect file had been compared to the hash value of a known file, and that a report was made by Google because it suspected the file contained child pornography based upon the hash value comparison. Therefore, the Defendant has failed to establish an "intentional" error or a reckless disregard for the truth and the evidence should not be suppressed.

C. The *Leon* "Good Faith Exception" Applies.

In the event the Court finds a violation of the Fourth Amendment protection against search and seizure because the affidavit was not supported by probable cause, this Court can also find that the good-faith exception applies in this case. The test for good-faith is set forth in *United States v. Leon*, 468 U.S. 897 (1984) as follows:

> Even if a search warrant is deemed invalid, evidence obtained pursuant to the warrant is not automatically suppressed. Such evidence is admissible when it is objectively reasonable for a police

> officer to have relied in good faith on the issuing judge's probable-cause determination. *Leon*, 468 U.S. at 922, 104 S.Ct. 3405. This "good-faith inquiry is confined to the objectively ascertainable question whether a reasonably well trained officer would have known that the search was illegal despite the [issuing judge's] authorization." *Id.* at 922 n. 23, 104 S.Ct. 3405. The rationale for such an exception is that no justification exists to exclude evidence "when an officer acting with objective good faith has obtained a search warrant from a judge or magistrate and acted within its scope." *Id.* at 920, 104 S.Ct. 3405.

United States v. Puckett, 466 F.3d 626, 629-630 (8th Cir. 2006).

In this case, the search warrant or Affidavit does not contain any information which would lead an officer to believe that the search was invalid. Furthermore, even if it is determined that there was no probable cause to issue the search warrant, the *Leon* good-faith exception applies to this case. Under the *Leon* good faith exception:

> disputed evidence will be admitted if it was objectively reasonable for the officer executing a search warrant to have relied in good faith on the judge's determination that there was probable cause to issue the warrant. In assessing whether the officer relied in good faith on the validity of a warrant, we consider the totality of the circumstances, **including any information known to the officer but not included in the affidavit**, and we confine our inquiry 'to the objectively ascertainable question whether a reasonably well trained officer would have known that the search was illegal despite the [issuing judge's] authorization.'

United States v. Grant, 490 F.3d 627, 632 (8th Cir. 2007) (emphasis added) (quoting *Leon*, 468 U.S. at 922, n. 23) (internal citations omitted).

The evidence at the suppression hearing will establish that it was objectively reasonable for Agent Aramayo to believe that the file sent from Google was suspected of containing child pornography.

CONCLUSION

The Affidavit contains probable cause and, despite the Defendant's claims to the contrary, does not contain false statements or omissions of material fact. The United States requests that Hedrick's motion to suppress be denied.

Dated this 18th day of October, 2019.

RONALD A. PARSONS, JR.
United States Attorney

/s/ Jeffrey C. Clapper

Jeffrey C. Clapper
Assistant United States Attorney
P.O. Box 2638
Sioux Falls, SD 57101-2638
Telephone: (605)357-2351
Facsimile: (605)330-4410
E-Mail: jeff.clapper@usdoj.gov